

Esteganografía

Álvaro Navarro Clemente
anavarro@gsync.escet.urjc.es
Universidad Rey Juan Carlos, Móstoles, España

Junio del 2005

1. Introducción

Estimar una definición universal para el concepto de seguridad informática se nos antoja bastante difícil. La dificultad radica en la naturaleza tan relativa que hacen de la seguridad un término heterogéneo dependiendo del punto de vista del que se mire. Atendiendo a la *wikipedia* podemos definir seguridad informática como todos los mecanismos y métodos para asegurar la integridad, confidencialidad y accesibilidad (C.I.A) de un conjunto de datos. Dichos datos deben ser protegidos de algún daño durante su tratamiento normal, y los procesos habituales debe ser conservadores con los datos sin destruir la información, salvo cuando ésta sea su misión expresa.

Por tanto si queremos tener una seguridad más o menos eficiente en un sistema, debemos asegurarnos que se deben cumplir las tres premisas anteriormente citadas (C.I.A) intentado tener el sistema libre de **amenazas**. Pero, ¿Qué tipo de amenazas? El siguiente apartado recoge una serie de amenazas típicas, las cuales pueden aprovechar las **vulnerabilidades**, deficiencias o errores, que tengamos en nuestro sistema para que, mediante un **ataque** consigan poner en riesgo nuestro sistema.

Centrándonos en la confidencialidad, una de las premisas que más nos interesa es que una tercera persona no autorizada, pueda interceptar nuestro mensaje, leerlo y por qué no, modificarlo. Es aquí donde se hace necesaria la aparición de técnicas que eviten que alguien pueda saber el mensaje que intentamos transmitir. La técnica más comunes son la **criptografía** y la **textbfesteganografía**, las cuales se encargan de formar un nuevo mensaje, ilegible para una tercera persona, y que receptor y emisor saben interpretar.

De acuerdo a algunas definiciones, esteganografía es el arte de cifrar, o en caracteres, que no son inteligibles excepto a personas que tienen la clave(criptografía). En términos computacionales, la esteganografía ha evolucionado en la práctica de esconder un mensaje en uno más grande de forma que los demás no puedan saber de la presencia o contenidos del mensaje oculto. Actualmente, la esteganografía ha evolucionado en la forma de esconder un archivo en forma de multimedia, como una imagen, un archivo de audio (.wav o .mp3) o incluso un archivo de video.

La esteganografía puede ser usada para una variedad de propósitos, algunos buenos, y algunos no tan buenos. Los propósitos legítimos pueden incluir cosas como marcado de agua de imágenes

por razones como protección de derechos de autor. Puede ser usada para mantener la confidencialidad de información valiosa, proteger los datos de posible sabotaje, robo o vistas no autorizadas.

Desafortunadamente, la esteganografía también puede ser usada para razones no legítimas. Si alguien estaba tratando de robar datos, éstos podrían ser enviados de manera aparentemente inocente a través de una imagen en un e-mail. Por tanto, un sospechoso podría ocultar evidencia a través de esteganografía.

2. Historia de la esteganografía

La historia ha proporcionado incontables situaciones por la que la información haya tenido que atravesar el territorio hostil o enemigo para alcanzar su destino. La gente ha usado diferentes métodos, algunos ingeniosos, para encubrir la información y que con el paso del tiempo fueron mejorando.

En la Grecia antigua, usaban un método mediante el cual, una persona elegida al azar y con la cabeza afeitada, le tatuaban el mensaje secreto en la cabeza, tras lo cual le dejaban crecer el pelo a su longitud normal. El mensajero procedería a llevar a su destino el mensaje ya que pasaría cualquier control de seguridad al no percibir nada sospechoso por parte del enemigo. Una vez presentado al receptor de la información, éste le afeitaría la cabeza para leer el texto secreto. Una desventaja importante a este método era el estado latente en conseguir el mensaje al receptor. Se tuvo que esperar a que el pelo creciera suficientemente para cubrir el texto antes de que el mensaje pudiera ser entregado. Otra desventaja a este método es que el mensajero quedaba marcado con el tatuaje de por vida sin poder ser destruido.

Otro método usado en Grecia antigua eran las tabletas cubiertas de cera. La cera era raspada de la tableta, quedando el mensaje escrito en la madera debajo para posteriormente volver a aplicar otra capa de cera para cubrir el mensaje. El receptor de la tableta rasparía la cera de nuevo para revelar el mensaje.

Durante la guerra mundial II, las tintas invisibles fueron utilizadas para encubrir la información en notas o letras aparentemente estándares e inofensivas. Las fuentes comunes para las tintas invisibles son leche, vinagre, zumos de fruta y orina.

Uno de los métodos más ingeniosos está desarrollado por Gaspar Schott y se detalla en su libro *Schola Steganographica*. El método implicaba el codificar la información emparejando letras a las notas musicales específicas sobre una hoja. Aparentemente aparecería como una partitura musical normal. Si uno tocara el trozo de dicha partitura musical en un instrumento, el resultado no sería todo lo agradable que esperaríamos a priori.

2.1. Cómo funciona la esteganografía

Para esconder un mensaje mediante esteganografía, en primer lugar se escoge un fichero cualquiera, un documento Word, un documento PDF de Adobe, un fichero de imagen BMP o uno de sonido .WAV o .MP3, y se escoge el mensaje que se quiere ocultar, un mensaje de texto u otro fichero. El programa encriptador modifica el portador de varias formas posibles: alterando los valores de algunos de los puntos de la imagen, sumándoles o restándoles uno (+1 para indicar el

bit 1, por ejemplo, y -1 para indicar el bit 0), de forma que sea imperceptible al usuario, pero que alguien que sepa que en esa imagen hay un mensaje, pueda recuperarlo. Existen otros métodos para ocultar información que serán estudiados más adelante

La siguiente figura muestra cómo funciona, a grandes rasgos, la esteganografía:

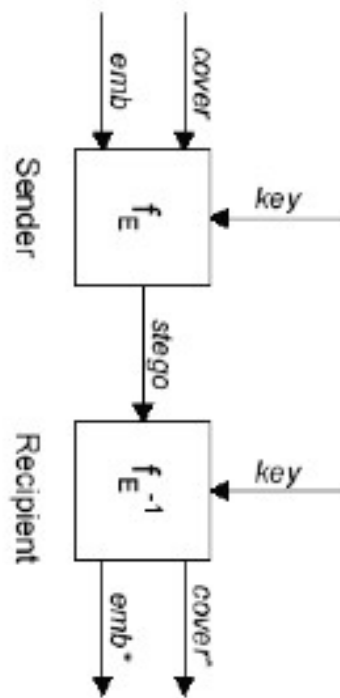


Figura 1: funcionamiento del algoritmo de esteganografía

- f_E = Función para embeber
- $f_{E^{-1}}$ = Función para extraer
- cover = Objeto donde embeber el mensaje (foto, audio o video)
- emb = Mensaje embebido
- key = Parámetro de f_E
- stego = Objeto con el mensaje embebido
- sender = Emisor
- recipient = Receptor

Actualmente hay tres técnicas para hacer esteganografía:

- Sustitución.
- Inyección.
- Generación de nuevos ficheros.

2.2. Método de Sustitución

Cada fichero que es creado contiene áreas de datos no usadas o que no son importantes. Estas áreas pueden ser reemplazadas sin aparentes cambios visuales o estructurales del fichero original. Ésto permite esconder información sensible dentro del fichero y tener aún la certeza que el fichero original no ha sufrido ninguna mutación. El método del *bit menos significativo* (LSB) sustituye el último bit de cada byte, de tal forma que podemos repetir este proceso con cada byte sin que el ojo humano aprecie diferencia alguna.

Podemos ver un ejemplo en la siguiente secuencia. Tenemos un grupo de bytes representando un color dentro de un foto, este conjunto de bytes podría ser representado de la siguiente forma:

- 10010110 01101010 11100101

Así representamos una imagen de 24 bits (3 bytes x 8 bits). Supongamos que cambiamos el primer bit (1) de la primera palabra. Siendo el más significativo, significa que el cambio sí tendría efectos visuales sobre la imagen original. Sin embargo, si cambiamos el último bit de la palabra, los efectos no serán apreciables.

El método LSB funciona mejor en fichero que tengan *ruido*, es decir, fotos que tengan muchos colores y figuras, así como fichero de audio que tengan diferentes cambios de frecuencias. Por tanto, cuanto más *ruido* tengo al fichero más difícil será que una persona sea consciente de la manipulación realizada.

El método de sustitución no incrementa el tamaño de la imagen sin embargo debemos tener en cuanto el tamaño del mensaje que queremos ocultar. Así pues, este método es utilizado debido a su rapidez y facilidad de uso.

2.3. Método de Inyección

El método de inyección implica encajar el mensaje secreto directamente en el objeto portador. El problema reside en que generalmente ésto hace que el fichero crezca de tamaño que el fichero original. Si bien, no es un factor determinante (ya que una tercera persona no tiene por qué tener el fichero original), sí hace que sea una desventaja frente a otros métodos.

2.4. Método de generación de un nuevo fichero

Esta técnica implica el coger el mensaje y usarlo para generar un nuevo fichero desde la nada. Una de las ventajas de este método es que no existe un fichero *original* con el que comparar.

Existen varios ejemplos que usan esta técnica:

- El problema del prisionero. Gus Simmons describe a dos personas: Alice y Bob quienes han sido arrestados y separados en diferentes celdas. Su objetivo es comunicarse para planear la escapada pero sin que el guardián, de nombre Willie, lo perciba. Además Willie no permite ningún contacto entre ellos para no facilitarse información secreta. Así pues Bob dibuja un cuadro inofensivo que contiene los colores y patrones específicos que Alicia interpretará como un mensaje. Willie mirará el cuadro y pensará que dicho objeto es totalmente inofensivo y pasará inocentemente el dibujo a Alice.
- *Spam Mimic*: es una aplicación web que cogerá el secreto que queramos pasarle y lo codificará mediante un mensaje de *spam* que aparentemente no se diferencia de cualquier otro mensaje de este tipo que circula por Internet. La URL del sitio web es <http://www.spammimic.com>

3. Elección del portador

¿Qué formato digital deberíamos elegir para portar nuestro mensaje secreto? La esteganografía puede ser usada en prácticamente casi cualquier tipo de fichero. En este apartado sólo trataremos los métodos más comunes usados en imágenes, audio y vídeo.

3.1. Imágenes

Los métodos más comunes para ocultar información en una imagen son:

- Bit Menos significativo. La base teórica es la misma comentada en la sección anterior, así que nos limitaremos a aplicar dicha teoría al mundo de las imágenes. Para un ordenador una imagen no es más que un array de números que representan intensidades de luz en varios puntos, denominados píxel. Por tanto en la representación de cada píxel la codificación binaria dependerá en cierta medida del peso de sus bits. Si aprovechamos el bit menos significativo para almacenar información en todas las palabras que forman la imagen, obtendremos un mensaje oculto sin que la imagen final difiera prácticamente de la original.
- Máscara. La compresión de una imagen puede, en ocasiones, tener efectos en la integridad final del mensaje oculto. Existen dos tipos de compresiones:
 - *Lossy*, usado por el famoso formato JPEG
 - *Lossless*, usados por los formatos BMP y GIF.

Una simple conversión de GIF a BMP a otro tipo de compresión como por ejemplo JPEG, puede ser que haya información oculta que podría ser destruida. El enmascaramiento y el filtrado son técnicas más efectivas que la anterior, LSB, sobre todo a la hora de usar formatos JPEG.

3.2. Audio

El odio humano es extremadamente sensible a cambio en los patrones de audio, pero no tanto como para percibir cambios dentro de una misma frecuencia. A la hora de ocultar un mensaje en audio, es importante saber el medio por el que se va a transmitir el mensaje, ya que no es lo mismo entre medios digital-digital (entre ordenadores) o entre aire-digital (microfono). Cuando se quiere ocultar información sensible dentro de un fichero de sonido, se suelen utilizar las siguientes cuatro técnicas:

- Codificación *Low-Bit*. El mensaje puede ser almacenado en ficheros de sonido de la misma manera que la técnica LSB hace con las imágenes
- *Spread Spectrum*. Es el método de ocultar un mensaje de baja señal dentro de otro de señal mayor. Este método añade ruido aleatorio para completar perfectamente la ocultación final.
- *Echo Data Hiding*. Este método usa el eco de un fichero de sonido para ocultar en él la información secreta.
- *Máscara perceptual*. Este método usa el concepto de ocultar un sonido tras otro de la misma frecuencia.

3.3. Video

Cuando queremos ocultar información en vídeos se suele utilizar el llamado método de *Discrete cosine Transform*. Un buen ejemplo de este método podría ser la videoconferencia, el cual requiere una tasa muy alta de información que viajará a través de la red. Para solucionar este alto consumo, el video a transmitir se suele comprimir de tal forma que sólo se transmiten las diferentes entre *frame* y *frame*. Es aquí donde podemos aprovechar la información transmitida para realizar esteganografía.

4. Esteganálisis

Esteganálisis es la técnica mediante la cual se identifica un mensaje oculto dentro de un medio. Tendremos dos tipos de ataques: ataques pasivos y ataques activos. A continuación se detallan ambos métodos.

4.1. Ataque activo

Este tipo de ataques implican el destruir el mensaje ocultado. Es muy frecuente en tecnologías con *marcas de agua* digitales donde el principal objetivo es inutilizar dichas marcas. Los ataques activos también son útiles en situaciones donde se sospecha que existe esteganografía pero que el mensaje ocultado no es importante. Un buen ejemplo son las imágenes donde se pueden aplicar algún efecto digital sin que lo perciba el ojo humano pero que modificará el mensaje oculto que está embebido en la imagen dejándolo totalmente irrecuperable.

4.2. Ataque pasivo

Un ataque pasivo implica la detección del uso de esteganografía y es una forma de descifrar los mensajes ocultos. Los tipos de ataques incluyen:

- Visionado del fichero
- Escuchas del fichero
- Ejecución de comparaciones en un fichero (si se tiene el fichero original)
- Ataques estadísticos. Éstos implican la detección de cambios en los patrones de los píxeles de los Bits Menos Significativos (LSB)
- Firma

Obviamente los dos primeros métodos del análisis no devolverán resultados exactos. El propósito de la esteganografía es que los cambios estén ocultos. Por lo tanto simplemente viendo o escuchando el archivo no significa revelar el mensaje secreto. Los primeros cuatro métodos implican el realizar comparaciones contra el archivo original (esto puede indicar a menudo que un archivo es portador del mensaje oculto y por lo tanto ser acertado).

Si en la esteganografía se utiliza el método *The Right Way*, es porque el atacante no tiene acceso al archivo original sin modificar. Si una persona quiere utilizar esteganografía para ocultar un mensaje secreto, sería absurdo utilizar un archivo bien conocido o fácilmente disponible para encubrir el mensaje dentro. El sentido común nos dice que lo mejor es utilizar un archivo que nunca antes haya sido visto por cualquier persona o por lo menos, que haya sido elegido de una localización poco conocida dentro de Internet.

5. herramientas

La clasificación de las diferentes herramientas utilizadas, se ha hecho atendiendo al sistema operativo. En concreto se han probado herramientas de UNIX, Macintosh y Windows. Al final de la sección se incluye una tabla resumen con una valoración atendiendo a la potencia de la herramienta, la facilidad de uso y su accesibilidad de cara al usuario final.

5.1. Esteganografía en Windows

- **Steganos Security Suite:** Se trata de una de las herramientas más completas de seguridad. Entre las pruebas que se pueden realizar incluyen ocultación de unidades virtuales, información crítica en imágenes y música. La herramienta se completa con herramienta antitroyanos y spyware, protección frente ataques denial of service y un completo password manager. Entre las pruebas realizadas, destaca la ocultación de un mensaje secreto dentro de una imagen. Los resultados son los mostrados en las figuras 2 y 3.



Figura 2: Steganos Security. Fotografía de origen



Figura 3: Steganos Security. Fotografía final